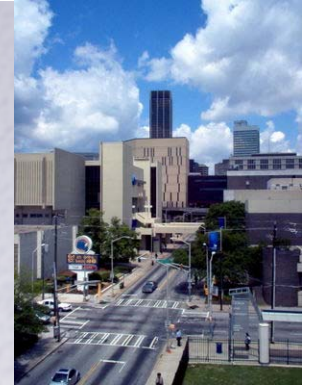


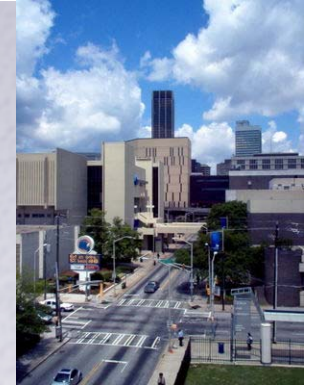
eFortresses, Inc. - ISO 27001:2005 - GSU's Roadmap For a World Class Information Security Management System

*William Monahan, Lead Information Security
Administrator, Georgia State University*

*Taiye Lambo, CTO and Founder,
eFortresses.com*



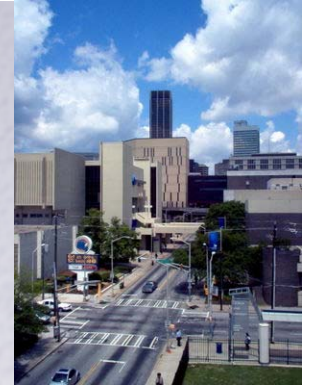
Today's Agenda



- Prerequisites For Success
- Risk Management
- PDCA Model
- Establishing and Operating an ISMS
- Evaluating and Measuring an ISMS
- Certifying under ISO 27001:2005
- Governance Training



Prerequisites For Success



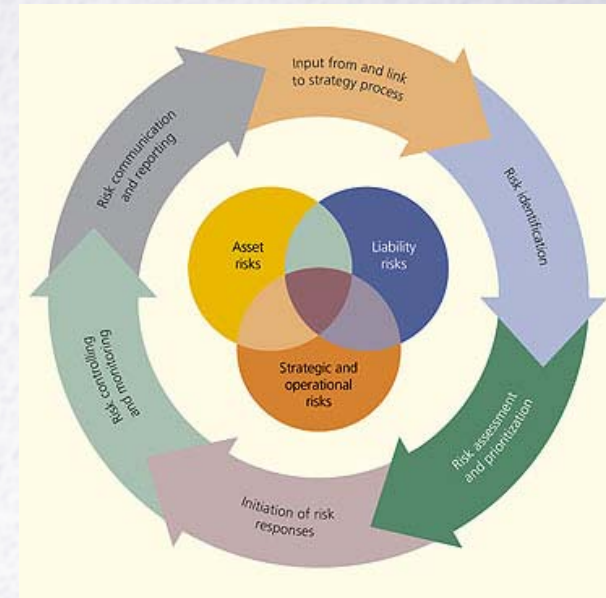
- We believe that the following are critical success factors:
 - Top Management Support
 - Collaborations with Key Enterprise Stakeholders
 - Understanding of key strategic business goals & objectives



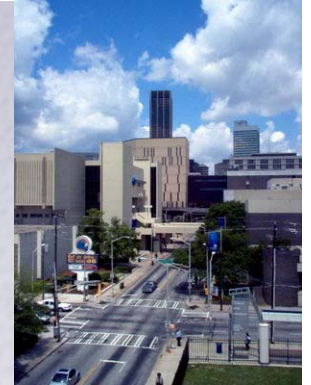
Risk Management



- Risk Management Process Model
- Asset Identification and Classification
- Risk Assessment Methodology
- ISO 17799/27001 Annex A
- Risk Treatment



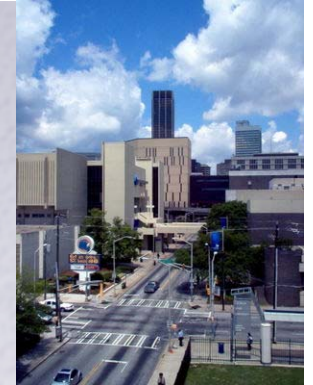
Risk Management Process Model



- Assess and evaluate risks
- Select, implement and operate controls to treat risks
- Monitor and review risks
- Maintain and improve risk controls



Identification of Assets



- Inventory and classification
- Identify legal and business requirements relevant to the assets
- Valuation of identified assets taking requirements into account as well as impacts of loss of C.I.A.
- Identify threats and vulnerabilities
- Assessment of likelihood threats will result in vulnerabilities getting exploited
- Calculate risk
- Evaluate risks against a pre-defined risk scale



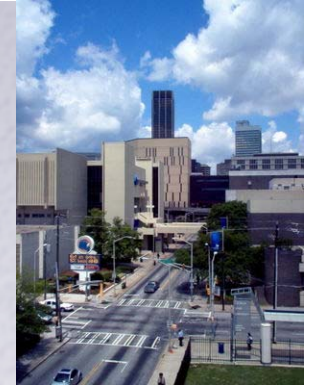
Risk Assessment Software



- Automated help with risk assessments and treatment plans
 - Proteus Enterprise: <http://infogov.co.uk>
Modular web based compliance, information security risk management and governance solution aimed at large enterprises. Brings together and links controls, compliance, business impact analysis, risk analysis, documentation and incident management into one comprehensive solution. Includes a business intelligence dashboard and reporting capability.



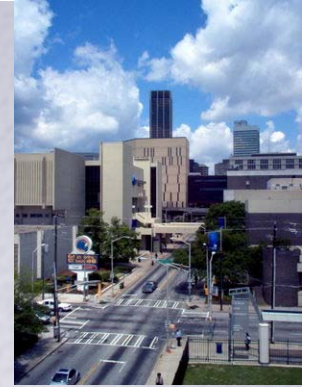
ISO 17799/27001 Controls



- 133 Separate Controls and 11 domains capturing all aspects of information security—a number of controls assist with implementing an ISMS
- ISO 27001:2005 describes what the requirements are under each control set
- ISO 17799:2005 contains guidance on how to implement these controls
- In completing your SOA (Statement of Applicability), you select the controls you plan to implement and/or exclude specific controls because they either don't apply to your business or you will accept the risk of not implementing them



Certification Process



Establish ISMS

Obtain Quotation

Apply for Certification

Pre-Audit

Certification Audit

Obtain Certificate

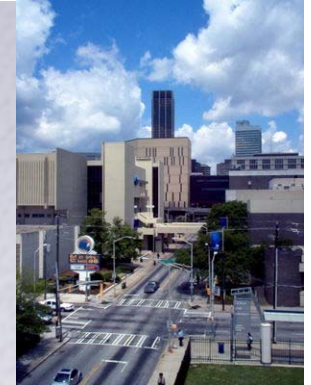
There are six critical steps in the ISO/IEC 27001:2005 certification process.

The level of activity required for each step varies by certification body.





PDCA Model

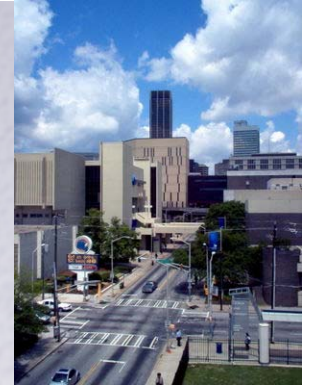


- Plan—Establish the ISMS
- Do—Implement and Operate the ISMS
- Check—Monitor and Review the ISMS
- Act—Maintain and Improve the ISMS



Step One:

Establishing and Operating an ISMS

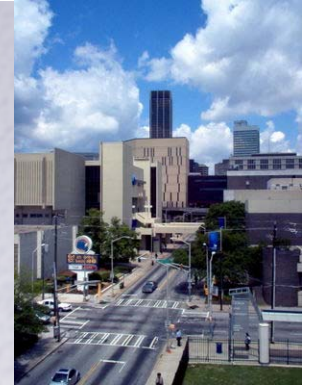


- Procure the ISO/IEC 27001:2005 standard.
- Obtain full executive management support.
- Define the Scope and Boundary of the ISMS.
- Define an ISMS Policy.



Step One (Cont):

Establishing and Operating an ISMS

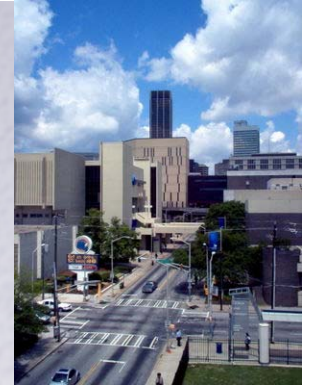


- Define the risk assessment approach.
- Identify, analyze and evaluate the risks.
- Identify and evaluate risk treatment options.
- Select controls and control objectives and reasons for selection.
- Obtain management approval of the proposed residual risks.
- Obtain management authorization to implement and operate ISMS.
- Prepare a “statement of applicability”.



Step One (Cont.):

Evaluating and Measuring an ISMS



- Execute monitoring and review procedures
- Review effectiveness of the ISMS
- Measure effectiveness of controls
- Conduct internal audits
- Management reviews
- Update security Plans
- Document results



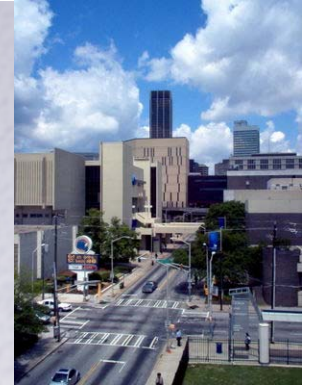
Step One (Cont.): Evaluating and Measuring an ISMS



- Implement identified improvements
- Take appropriate corrective and preventative actions
- Communicate actions and improvements to all interested parties
- Ensure improvements achieve intended objectives



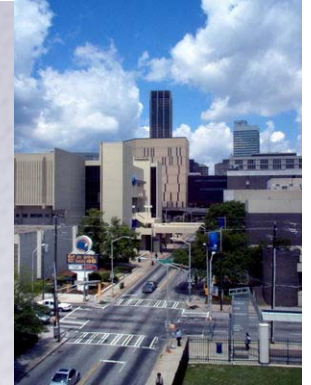
Step Two: Obtain Quotation



- Consider the following before requesting a quotation from an accredited certification body to carry out an audit of your ISMS:
 - Their experience in your industry.
 - Their technical capability and track record.
 - Their professional rapport with the consultant(s) assisting you to implement your ISMS.
 - Their location and global coverage.
 - Referral from existing customers.



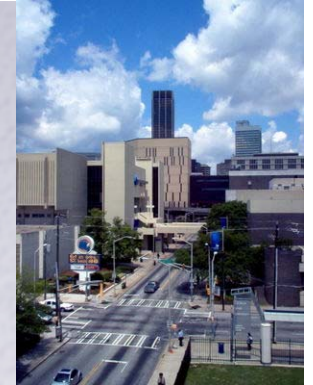
Step Three: Apply For Certification



- Consider the following before you apply for certification:
 - Readiness of your certification management committee.
 - Availability of key staff (process owners, management , etc.)
 - Current state of your ISMS, including any recent changes that may potentially impact the audit.
 - Duration of audit.



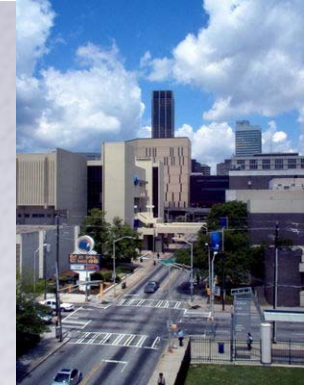
Step Four: Pre-Audit



- Ensure that you have the following for the Pre-Audit:
 - Management approved Security Policy and ISMS Manual, including approval & revision dates and approvers, plus evidence policies and procedures are being adhered to.
 - ISMS scope and boundaries
 - Documented Risk Assessment approach and RTP (Risk Treatment Plan)
 - Management approved Acceptable risk document.
 - Management approved "Statement of Applicability," including justification of controls and control objectives included and excluded.



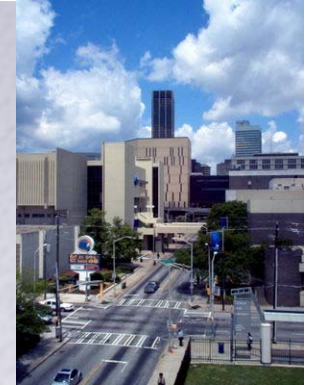
Step Five: Certification Audit



- Ensure that you have the following for the Audit:
 - Evidence of Management reviews and user awareness training.
 - Policies and Procedures and documentary proof that they are being adhered to.
 - Internal Audit procedure, including audit plan, schedule and industry certifications of team i.e. HISP, CISSP, CISM, CISA.
 - Procedure for measuring the effectiveness of ISMS, including a security metrics to measure effectiveness of all security processes.



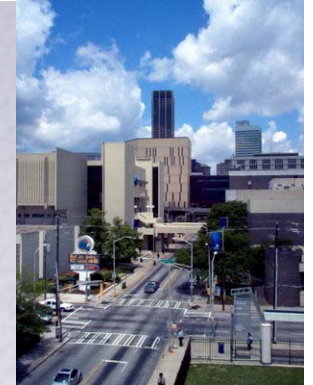
Step Five (Cont.): Certification Audit



- Ensure that you also have the following for the Audit:
 - A record of the management review of ISMS including evidence that corrective action(s) have been taken on previous observations.
 - Incident handling procedure and maintain records and evidences with root cause analysis.
 - Report of independent review or audit of processes by third party.
 - Full Disaster Recovery Plan or management approved roadmap for implementation.



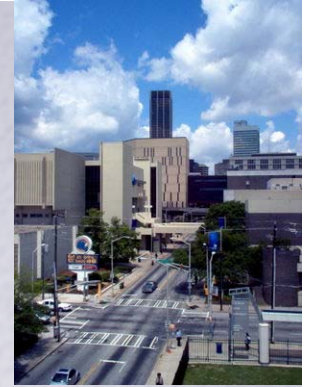
Step Six: Obtain Certificate



- Ensure the following:
 - The boundary of your ISMS is well defined on your ISO 27001 certificate and is fully understood by all stake holders.
 - The validity date of your ISO 27001 certificate is defined.
 - Frequency of the “surveillance audit” is agreed with your Certification Body.
 - Your marketing team clearly understands any limitations associated with your certificate.



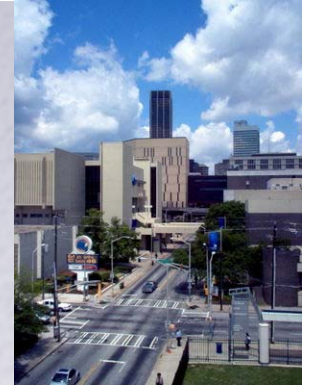
Governance Training



- BSI Americas ISO/IEC 27001:2005 Implementation Course
 - <http://www.bsiamericas.com/TrainingInformationSecurity/index.xalter>
- HISP (Holistic Information Security Practitioner) Training/Certification
 - <http://www.hispcertification.org>



Questions?



- ***References***

- ISO/IEC 27001:2005
- BS 7799-3:2006 (Risk Mgt)
- BIP 0071-0074 (ISMS Guidance Series from BSI)
- ISO/IEC 17799:2005 (Controls)

